



Systèmes
d'Exploitation

Didier Verna
EPITA

Généralités

Authentification

Attaques

Internes
Externes

Protection

Modèles
formels

Systèmes d'Exploitation

Protection et Sécurité

Didier Verna

didier@lrde.epita.fr
<http://www.lrde.epita.fr/~didier>



Table des matières

Systèmes
d'Exploitation

Didier Verna
EPITA

Généralités

Authentification

Attaques

Internes
Externes

Protection

Modèles
formels

1 Généralités

2 Authentification des utilisateurs

3 Attaques

- Internes
- Externes

4 Mécanismes de protection

5 Modèles formels



Protection $\neq$ sécurité

Systèmes
d'Exploitation

Didier Verna
EPITA

Généralités

Authentification

Attaques

Internes
Externes

Protection

Modèles
formels

- **Sécurité = définir une politique de fonctionnement**
(problème externe)
 - ▶ Notion politique, légale, administrative *etc.*
 - ▶ Problématique générale, prise en compte de l'environnement du système (sécurité physique, authentification des personnes *etc.*)
- **Protection = appliquer (implémenter) cette politique**
(problème interne)
 - ▶ Notion technique
 - ▶ Problématique du système d'exploitation (gestion et contrôle d'accès aux ressources *etc.*)
- **Remarque :** Les problèmes de protection et sécurité ne s'adressent plus qu'aux concepteurs de systèmes, mais aussi aux programmeurs et aux utilisateurs.



Les 3 problèmes de sécurité

Systèmes
d'Exploitation

Didier Verna
EPITA

Généralités

Authentification

Attaques

Internes

Externes

Protection

Modèles
formels

■ Nature des menaces

- ▶ Confidentialité / exposition
- ▶ Intégrité / corruption
- ▶ Disponibilité / déni de service (DoS)

■ Intrusions

- ▶ Passives (du p'tit curieux au vrai espion)
- ▶ Actives (du p'tit malin au vrai voleur)
- ▶ Non humaines (virus, vers *etc.*)

■ Perte accidentelle de données

- ▶ Impondérables (feux, inondations *etc.*)
- ▶ Dysfonctionnement technique (disques, bugs *etc.*)
- ▶ Erreurs humaines (`rm -fr` *etc.*)



Authentification $\neq$ identification

Systèmes
d'Exploitation

Didier Verna
EPITA

Généralités

Authentification

Attaques

Internes
Externes

Protection

Modèles
formels

■ Outils

- ▶ **Connaissances utilisateur** : identificateur, mot de passe, phrase de passe *etc.*
- ▶ **Possessions utilisateur** : clé, carte magnétique, carte à puce, « smart card » (8bit, 4MHz, 16K ROM, 8K EEPROM, 512b RAM, 9600bps) *etc.*
- ▶ **Attributs utilisateur** : empreinte digitale, rétinienne, vocale, signature *etc.*, tout en restant psychologiquement acceptable pour les usagers.

■ Contre-mesures

- ▶ Tout enregistrer
- ▶ Protection par « callback »
- ▶ Piéger le système



Le drame des mots de passe

Systèmes
d'Exploitation

Didier Verna
EPITA

Généralités

Authentification

Attaques

Internes
Externes

Protection

Modèles
formels

■ Faiblesses

- ▶ **Exposition intentionnelle** : Transfert à un tiers, postit *etc.*
- ▶ **Exposition accidentelle** : Surveillance visuelle, vidéo, informatique
- ▶ **Découverte par test** : connaissance de l'utilisateur (mots de passe trop évidents : 80%), force brute (dictionnaires)

■ Mesures préventives

- ▶ Interdire les mots de passe trop simples
- ▶ Changer les mots de passe à intervalles réguliers
- ▶ Encrypter les transmissions
- ▶ Stocker et cacher les formes encryptées
- ▶ Le silence est d'or



Attaques internes

Systèmes
d'Exploitation

Didier Verna
EPITA

Généralités

Authentification

Attaques

Internes

Externes

Protection

Modèles
formels

- **Cheval de Troie** : code malveillant dans une coquille bénigne.
 - ▶ **Unix** : attention au PATH, aux typos *etc.*
 - ▶ **Windows** : `.exe` récupérés sur l'internet, `.exe` vs. `.com`, raccourcis du bureau *etc.*
- **Login spoofing** : vrai-faux écran de login. Seule protection : forcer une séquence clavier non récupérable (ex. CTRL-ALT-DEL)
- **Bombe logique** : se déclenche par *absence* d'intervention
- **Porte de contournement** : (backdoor, trapdoor, « passer par derrière »). Contourner les procédures normales de sécurité pour un utilisateur précis.



Attaques internes (suite)

Systèmes
d'Exploitation

Didier Verna
EPITA

Généralités

Authentification

Attaques

Internes

Externes

Protection

Modèles
formels

- **Défauts de programmation** : avec des langages non sûrs (ex. débordements de buffers en C)
- **Défauts de conception** :
 - ▶ **Unix** :
 - `lpr` avait une option pour effacer les fichiers après impression *etc.*
 - `ln -s /etc/passwd core.`
 - ▶ **TENEX** : (DEC-10). Craquage de mots de passe en $128n$ au lieu de 128^n (callback utilisateur sur les défauts de page)



Attaques externes

Systèmes
d'Exploitation

Didier Verna
EPITA

Généralités

Authentification

Attaques

Internes

Externes

Protection

Modèles
formels

- **Virus** : fragment de code intégré dans un programme légitime. Reproduction par contamination d'autres programmes. Aucun antivirus universel : les antivirus évoluent en même temps que les virus.
- **Vers** : programme autonome et auto-reproducteur. Consommation (voire épuisement) des ressources systèmes. Dissémination à travers les réseaux informatiques.



Virus

Systèmes
d'Exploitation

Didier Verna
EPITA

Généralités

Authentification

Attaques

Internes

Externes

Protection

Modèles
formels

- **Exécutables** : « virus de remplacement » (écrasent des programmes avec eux-mêmes), « virus parasites » (s'attachent à des programmes, en tête, en queue, ou dans des cavités).
- **Résidents** : caché en RAM en permanence. Redirection de `trap`, attendre un `exec` *etc.*
- **Boot sector** : exécutés avant même le chargement du système. Point de départ fréquent des virus résidents.
- **Pilotes** : chargés « officiellement » par le système, exécutés en mode noyau.
- **Macros / scripts** : VB dans Office, ELisp dans Emacs *etc.* Transmission par mail croissante. Peu de qualifications requises.
- **Source** : contaminent les sources plutôt que les exécutables.



Propagation

Systèmes
d'Exploitation

Didier Verna
EPITA

Généralités

Authentification

Attaques

Internes

Externes

Protection

Modèles
formels

- Freewares, sharewares sur le web
- Floppies, zips, clés USB *etc.*
- Internet, LAN *etc.*
- Mails news (attachements, carnets d'adresses)
- Plugins pour les navigateurs
- *etc.*

⇒ **Éduquer les utilisateurs !!** (de Windows)



Techniques anti-(anti-(...)) virales

Systèmes
d'Exploitation

Didier Verna
EPITA

Généralités

Authentification

Attaques

Internes

Externes

Protection

Modèles
formels

- **Scanners** : comparaison de tous les exécutables avec une base de données. Mises à jour régulière.
 - ▶ Recherche floue (plus coûteuse, risque de fausses alarmes).
 - Préserver les dates originales des fichiers infectés, leur longueur (compression), se différencier des bases de données (encryption)
 - La procédure de décryptage ne peut pas être encryptée
 - Virus polymorphes (moteur de mutation)
- **Vérificateurs d'intégrité** : calcul (puis comparaison) de sommes de contrôle à partir d'un état sain
 - ▶ Écraser les sommes avec les nouvelles
 - ▶ Encrypter les sommes (avec une clé externe)
- **Vérificateurs de comportement** : antivirus résidents. Travail difficile.



Le vers de Morris

Systèmes
d'Exploitation

Didier Verna
EPITA

Généralités

Authentification

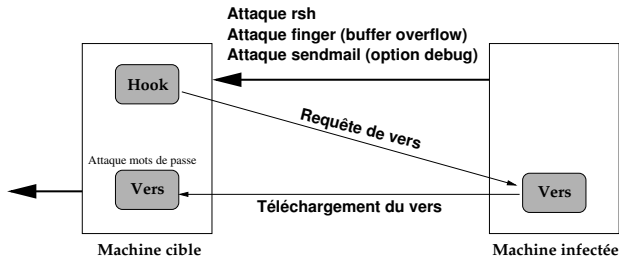
Attaques

Internes

Externes

Protection

Modèles
formels



- Lancé le soir du 2 Novembre 1988, détecté pour cause de DoS, solutions proposées le 3, neutralisé en quelques jours.
- *rtm* fait la une du New York Times à cause d'un ami *etc.*
- Polémiques autour de sa condamnation, création du CERT (Computer Emergency Response Team).



■ Un système informatique est

- ▶ Un ensemble de processus
- ▶ Un ensemble d'objets matériels (CPU, mémoire *etc.*)
- ▶ Un ensemble d'objets logiciels (programmes, fichiers *etc.*)
- ▶ Un ensemble d'opérations processus → objet
(les opérations peuvent dépendre des objets)

■ Principe de « nécessité d'accès »

- ▶ Restreindre l'accès aux seules ressources nécessaires
- ▶ Restreindre l'accès aux seules opérations nécessaires



Notion de domaine de protection

Systèmes
d'Exploitation

Didier Verna
EPITA

Généralités

Authentification

Attaques

Internes
Externes

Protection

Modèles
formels

■ Définitions

- ▶ **Droit d'accès** : paire (objet / ensemble de droits)
 $(O, \{D_1, D_2, \dots\})$
- ▶ **Domaine** : ensemble de droits d'accès
 $\{DA_1, DA_2, \dots\}$

■ Remarques

- ▶ Les domaines ne sont pas forcément disjoints
- ▶ Chaque processus s'exécute dans un domaine

■ Liaison processus / domaine

- ▶ **Statique** : ensemble de ressources disponibles fixe. Le principe de nécessité d'accès requiert un mécanisme de modification des contenus de domaines.
- ▶ **Dynamique** : requiert un mécanisme de « commutation de domaine » (pas nécessairement de modification).



Réalisation de domaines

Systèmes
d'Exploitation

Didier Verna
EPITA

Généralités

Authentification

Attaques

Internes
Externes

Protection

Modèles
formels

- **Domaine = Utilisateur** : les objets auxquels on peut accéder dépendent de l'utilisateur qui y accède.
Commutation de domaine au changement d'utilisateur.
 - ▶ **Unix** : Bit « setuid » (root) : indique un éventuel changement d'identité pour les accès (privilegiés).
- **Domaine = Processus** : les objets auxquels on peut accéder dépendent du processus qui y accède.
Commutation de domaine à la commutation de contexte.
- **Domaine = Procédure** : les objets auxquels on peut accéder correspondent aux variables utilisées par la procédure. Commutation de domaine à chaque appel de procédure.
 - ▶ **Multics** : 7 domaines de protection organisés en anneaux (par quantité de privilèges).
 - Espace d'adressage segmenté
 - « Liste de guichets » : points d'entrée par anneaux



Matrice de droits

Systèmes
d'Exploitation

Didier Verna
EPITA

Généralités

Authentification

Attaques

Internes
Externes

Protection

Modèles
formels

■ Définition

- ▶ Matrice domaine / objet $[D_i, O_j]$ contenant les droits
- ▶ Domaine d'exécution d'un processus choisi par le système d'exploitation
- ▶ Droits (D_i, O_j) spécifiés par les utilisateurs

■ Entrées particulières

- ▶ **Commutation de domaine** : les domaines sont vus comme des objets
- ▶ **Modification de droits** : les entrées (D_i, O_j) sont vues comme des objets



Implémentation de la matrice de droits

Systèmes
d'Exploitation

Didier Verna
EPITA

Généralités

Authentification

Attaques

Internes
Externes

Protection

Modèles
formels

- **Complète** : table globale en mémoire. Grande taille, matrice creuse.
- **Par colonne** : « ACL » (Access Control List). Pour chaque objet : liste de paires domaines (utilisateurs) / droits non vides. Extension par listes de droits par défaut.
- **Par ligne** : « Capacités de domaines ». Pour chaque domaine (processus) : liste de paires objets / droits non vides.



Rions un peu

Systèmes
d'Exploitation

Didier Verna
EPITA

Généralités

Authentification

Attaques

Internes
Externes

Protection

Modèles
formels

■ Orange Book

- ▶ Classification du Département Américain de la Défense (7 niveaux de sécurité)
- ▶ Windows obtient 0/7
- ▶ Unix obtient 2/7

■ Pourquoi les systèmes actuels sont-ils si peu sûrs ?

- ▶ Coût (conception et réalisation)
- ▶ Charge (temps administratif humain et CPU)
- ▶ Rétro-compatibilité (pression commerciale, utilisateurs)
- ▶ Fonctionnalités et sécurité sont contradictoires (« keep it simple »)



Sécurité multi-niveau

Systèmes
d'Exploitation

Didier Verna
EPITA

Généralités

Authentification

Attaques

Internes

Externes

Protection

Modèles
formels

- **Idée** : Contrôle d'accès sous l'égide du système plutôt que des utilisateurs (régulation du flot d'information plutôt que de l'information elle-même).
- **Sécurité : Bell / La Padula**
 - ▶ Un processus ne peut lire des objets qu'à niveau inférieur ou égal au sien
 - ▶ Un processus ne peut écrire des objets qu'à niveau supérieur ou égal au sien
- **Intégrité : Biba**
 - ▶ Un processus ne peut écrire des objets qu'à niveau inférieur ou égal au sien
 - ▶ Un processus ne peut lire des objets qu'à niveau supérieur ou égal au sien



Covert channels

La fuite d'information est toujours possible...

Systèmes
d'Exploitation

Didier Verna
EPITA

Généralités

Authentification

Attaques

Internes
Externes

Protection

Modèles
formels

- `1 = « while (1); », 0 = sleep ();`
- (Dé)Vérouillage, test d'existence de fichier
- Réquisition / relâchement de périphériques
- Stéganographie
- *etc.*

